

UNCLASSIFIED



SAMSUNG ANDROID OS 15 BRING YOUR OWN APPROVED DEVICE (BYOAD) CONFIGURATION TABLES

22 April 2025

Developed by Samsung and DISA for the DOD

UNCLASSIFIED

LIST OF TABLES

	Page
Table 1: Configuration Policy Rules for BYOD	1
Table 2: KPE Equivalent APIs.....	4

Unified Endpoint Management (UEM) empowers enterprise IT administrators with powerful tools to centrally set up, deploy, secure, control, and maintain desktops, laptops, smartphones, tablets, wearables, and Internet of Things (IoT) devices. Samsung has collaborated with the leading UEM providers to ease the management of Samsung devices, which feature the Knox Platform for Enterprise (KPE). To set up Samsung devices using popular UEM platforms, navigate to: <https://docs.samsungknox.com/admin/uem/index.htm>.

All policies listed in the document are implemented using Android Enterprise (AE) APIs. If the management tool does not implement the AE policy, a KPE API may be available to use as a substitute either directly by the management tool or via Knox Service Plugin (KSP). In this situation, look for an “*” next to the AE API in the comment of the associated policy row, which indicates a KPE substitute is available. To keep these tables as simple as possible, substitute KPE APIs will not be listed in the tables here. Refer to [Table 2](#) in this document for the full list of available substitutions.

In some cases, a KPE API could be used to allow additional features while remaining STIG compliant. Details of this are provided in the comment of the associated policy row.

Table 1: Configuration Policy Rules for BYOD

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Device Enrollment Configuration	Default device enrollment	Fully managed, Work Profile for company-owned devices, Work Profile for personally owned devices	Work Profile for personally owned devices	KNOX-15-708800, KNOX-15-709900	Enroll device as an Android Enterprise device.
Device Password Policies	Minimum password quality	Unspecified, Something, Numeric, Numeric(Complex), Alphabetic, Alphanumeric, Complex	Numeric(Complex)	KNOX-15-705000	This allows for PIN code. API: setPasswordQuality Or setRequiredPasswordComplexity If the management tool does not support

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
					Numeric(Complex) but does support Numeric , KPE can be used to achieve STIG compliance. In this case, configure this policy with value Numeric and use an additional KPE policy (natively by management tool or via KSP) Maximum Numeric Sequence Length with value 4 .
Device Password Policies	Minimum password length	0+ characters	Six characters	KNOX-15-704900	API: setPasswordMinimumLength
Device Password Policies	Max password failures for local wipe	0+	10 attempts	KNOX-15-705300	API: setMaximumFailedPasswordsForWipe
Device Password Policies	Max time to screen lock	0+ minutes	15 minutes	KNOX-15-705100	API: setMaximumTimeToLock
Device Restrictions	Face recognition	Enable/Disable	Disable	KNOX-15-706100	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_FACE
Device Restrictions	Trust agents	Enable/Disable	Disable	KNOX-15-705200	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_TRUST_AGENTS Or setTrustAgentConfiguration
Work Profile Policy Management	Certificates		Include DOD certificates in work profile	KNOX-15-709000	API: installCaCert *

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Work Profile Policy Manager	Galaxy AI	Enable/Disable Cloud Processing	Disable	KNOX-15-705700	API: allowIntelligenceOnlineProcessing
Work Profile Policy Management	Certificate revocation checks	Enable/Disable	Enable	KNOX-15-709600	* KPE provides an API to check for Certificate revocation.
Work Profile Restrictions	List of approved apps listed in managed Google Play	List of apps	List only approved work apps	KNOX-15-705500, KNOX-15-705600	*
Work Profile Restrictions	Hide Certain Preinstalled Apps	App package name	Only allowed work apps	KNOX-15-709800	API: setApplicationHidden
Work Profile Restrictions	Configure Chrome Autofill	ON/OFF	"PasswordManager Enabled"="OFF" "AutofillAddressEnabled"="OFF" "AutofillCreditCard Enabled"="OFF"	KNOX-15-710000	API: setApplicationRestrictions
Work Profile Restrictions	Configure Autofill	Allow/Disallow	Disallow	KNOX-15-710100	API: addUserRestriction, DISALLOW_AUTOFILL
Work Profile Restrictions	Input Methods	List of packages	List only approved Input Method Editor apps	KNOX-15-710200	API: setPermittedInputMethods
Work Profile Restrictions	Unredacted notifications	Allow/Disallow	Disallow	KNOX-15-705800	API: setKeyguardDisabledFeatures, KEYGUARD_DISABLE_UNREDACTED_NOTIFICATIONS

Policy Group	Policy Rule	Options	Settings	Related Requirement	Comment
Work Profile Restrictions	Modify accounts	Allow/Disallow	Disallow	KNOX-15-709200, KNOX-15-707400	API: addUserRestriction, DISALLOW_MODIFY_ACCOUNTS *
Work Profile Restrictions	Cross profile copy/paste	Allow/Disallow	Disallow	KNOX-15-707900	API: addUserRestriction, DISALLOW_CROSS_PROFILE_COPY_PASTE
Work Profile Restrictions	Configure credentials	Allow/Disallow	Disallow	KNOX-15-708600	API: addUserRestriction, DISALLOW_CONFIG_CREDENTIALS *
Work Profile Restrictions	Install from unknown sources globally	Allow/Disallow	Disallow	KNOX-15-705400	API: addUserRestriction, DISALLOW_INSTALL_UNKNOWN_SOURCES_GLOBALLY *

Table 2: KPE Equivalent APIs

STIG LISTED AE API	Values	Available KPE Substitute API Available in Case of Management Tool Not Supporting AE API
addUserRestriction	DISALLOW_CONFIG_CREDENTIALS	CertificatePolicy allowUserRemoveCertificates
	DISALLOW_INSTALL_UNKNOWN_SOURCES_GLOBALLY	RestrictionPolicy setAllowNonMarketApps
	DISALLOW_MODIFY_ACCOUNTS	DeviceAccountPolicy addAccountsToAdditionBlackList
N/A	N/A	CertificatePolicy enableRevocationCheck
N/A	N/A	AdvancedRestrictionPolicy allowIntelligenceOnlineProcessing
installCaCert	DOD Root and Intermediate Certs	CertificateProvisioning installCertificateToKeystore

STIG LISTED AE API	Values	Available KPE Substitute API Available in Case of Management Tool Not Supporting AE API
managed Google Play	List only approved work apps	ApplicationPolicy addAppPackageNameToWhiteList, ApplicationPolicy addAppPackageNameToBlackList, ApplicationPolicy addAppSignatureToWhiteList, ApplicationPolicy addAppSignatureToBlackList
setBackupServiceEnabled	FALSE	RestrictionPolicy setBackup
setMaximumFailedPasswordsForWipe	10	BasePasswordPolicy setMaximumFailedPasswordsForWipe
setMaximumTimeToLock	900	BasePasswordPolicy setMaximumTimeToLock
setPasswordMinimumLength	6	BasePasswordPolicy setPasswordMinimumLength
setPasswordQuality	Numeric(Complex)	BasePasswordPolicy setPasswordQuality Alternatively: PasswordPolicy setMaximumNumericSequenceLength(2) with password quality of Numeric.